

Поперешняк С. В., кандидат фізико-математичних наук, доцент,
доцент кафедри інформатики та програмної інженерії
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
ORCID: 0000-0002-0531-9809

ЗАСТОСУВАННЯ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ДЛЯ ЕНЕРГОЕФЕКТИВНОГО КЕРУВАННЯ ІОТ-МЕРЕЖАМИ

У роботі запропоновано новий метод енергоефективного керування бездротовими ІоТ-мережами, заснований на використанні коротких псевдовипадкових послідовностей для узгодження часової активності вузлів. На відміну від класичних централізованих схем керування, запропонований підхід забезпечує децентралізовану самоорганізацію системи, у якій кожен вузол самостійно формує графік своєї роботи, використовуючи локальний генератор псевдовипадкових чисел. Така організація дозволяє досягти рівномірного розподілу активних інтервалів у часі, зменшити кількість колізій у радіоканалі, оптимізувати використання енергоресурсів і підвищити загальну стійкість мережі.

Розроблено інформаційну модель генератора псевдовипадкових послідовностей, адаптовану до обмежених обчислювальних ресурсів мікроконтролерів класу ІоТ-вузлів, а також схему локального узгодження шаблонів між пристроями без потреби у глобальному координаторі. Запропоновано алгоритм оновлення станів генератора, що забезпечує гнучке реагування мережі на зміни умов роботи та появу нових вузлів. У межах дослідження проаналізовано переваги стохастичної синхронізації над традиційними методами керування доступом до середовища передавання, а також показано можливість інтеграції підходу в існуючі комунікаційні протоколи ІоТ-мереж.

Практичне значення отриманих результатів полягає у створенні універсального методу, який може бути впроваджений у широкому спектрі сенсорних і моніторингових систем без зміни апаратної архітектури пристроїв. Розроблений підхід відкриває перспективи використання у сфері екологічного та техногенного моніторингу, аграрних ІоТ-платформах, системах «розумного міста», бездротових промислових мережах і мобільних автономних комплексах. Реалізація методу сприяє підвищенню ефективності використання енергоресурсів, стабільності обміну даними та тривалості автономної роботи пристроїв у розподіленому середовищі.

Ключові слова: ІоТ-мережі, енергоефективність, псевдовипадкові послідовності, децентралізоване керування, сенсорні вузли, самоорганізація, моніторинг, автономні системи.

Popereshnyak S. V. Application of Pseudo-Random Sequence Generators for Energy-Efficient Control of IoT Networks

The paper proposes a novel method for energy-efficient management of wireless IoT networks based on the use of short pseudo-random sequences to coordinate node activity in time. Unlike traditional centralized control schemes, the proposed approach enables decentralized self-organization of the network, where each node independently determines its operation schedule using a local pseudo-random number generator. Such an organization ensures a statistically uniform distribution of active intervals, reduces the number of collisions in the radio channel, optimizes energy consumption, and increases the overall stability of communication within the network.

An information model of the pseudo-random sequence generator adapted for low-power microcontrollers has been developed, as well as a local coordination mechanism that allows synchronization of node activity without a central coordinator or global time reference. The proposed state-update algorithm provides flexible adaptation to changes in network topology and traffic conditions. The paper discusses the advantages of stochastic synchronization compared to classical medium access control schemes and outlines the possibilities for integrating the method into existing IoT communication protocols.

The practical value of the research lies in the ability to apply the proposed method in a wide range of sensor and monitoring systems without hardware modification. The approach can be effectively implemented in environmental and industrial monitoring networks, agricultural IoT platforms, smart city systems, and autonomous wireless infrastructures. Its application contributes to reducing energy consumption, maintaining reliable data exchange, and extending the lifetime of distributed IoT devices operating under energy constraints.

Key words: IoT networks, energy efficiency, pseudo-random sequences, decentralized control, sensor nodes, self-organization, monitoring systems, autonomous devices.

Постановка проблеми. Інтернет речей стрімко розвивається, охоплюючи побутові, промислові та наукові системи, де десятки тисяч малопотужних пристроїв працюють автономно. Більшість вузлів мають обмежене енергоживлення, тому навіть незначне перевантаження радіоканалу або зайві цикли передачі даних можуть скоротити час їхньої роботи у кілька разів.

© С. В. Поперешняк, 2025

Стаття поширюється на умовах ліцензії CC BY 4.0

У практиці керування такими мережами часто застосовуються фіксовані або детерміновані схеми обміну – із заздалегідь визначеними часовими слотами. Проте ці схеми не враховують реальну динаміку трафіку, випадкові збурення або неузгодженість між вузлами. Як наслідок, виникають колізії, повторні передачі, додаткові енергетичні втрати.

Проблема посилюється в умовах децентралізованих IoT-середовищ, де немає центрального контролера і кожен вузол діє самостійно. Тут особливо важливо, щоб пристрої могли координувати свою активність без постійного обміну службовими повідомленнями. Одним із можливих шляхів є використання коротких псевдовипадкових послідовностей як керуючих шаблонів – коли часи пробудження або передачі даних визначаються не строго, а стохастично, але з контрольованою повторюваністю. Такий підхід потенційно дозволяє зменшити одночасність активності вузлів і, відповідно, споживання енергії.

Метою дослідження є розроблення підходу до енергоефективного керування вузлами IoT-мереж із використанням генераторів коротких псевдовипадкових послідовностей, який забезпечує збалансування навантаження радіоканалу та зниження загального енергоспоживання мережі без втрати стабільності зв'язку.

Для досягнення поставленої мети сформулюємо задачі дослідження:

- проаналізувати сучасні методи керування енергоспоживанням у бездротових IoT-мережах і виявити їхні обмеження;
- побудувати модель генератора псевдовипадкових послідовностей, придатного для реалізації в малопотужних мікроконтролерах;
- запропонувати схему узгодження псевдовипадкових шаблонів між вузлами без центрального координатора;
- провести експериментальне або імітаційне дослідження, щоб оцінити вплив запропонованого підходу на середній час активності вузлів, затримку передачі та надійність обміну;
- сформулювати рекомендації щодо практичного впровадження методу в сенсорних і моніторингових системах.

Використання псевдовипадкових шаблонів дозволяє зменшити енергоспоживання, скоротити колізії у каналі зв'язку та подовжити термін автономної роботи вузлів без зміни апаратної архітектури.

Метод може бути реалізований у простих мікроконтролерах і застосований у системах моніторингу навколишнього середовища, «розумних містах», промислових мережах і агротехнологічних платформах. Результати дослідження можуть стати основою для розроблення нових алгоритмів самоорганізації IoT-пристроїв у розподілених енергообмежених середовищах.

Аналіз останніх досліджень і публікацій. Проблематика енергоефективного функціонування бездротових IoT-мереж посідає провідне місце в сучасних дослідженнях, що зосереджуються на мінімізації енергоспоживання сенсорних вузлів і підвищенні надійності зв'язку в умовах обмежених ресурсів. У низці робіт [1–3] запропоновано архітектури енергоощадних мереж на основі адаптивного керування режимами роботи вузлів, що поєднують зниження частоти передачі з оптимізацією маршрутизації даних. Такі підходи дозволяють продовжити час автономної роботи пристроїв, проте переважно спираються на централізоване керування або фіксовані часові слоти.

Подальші дослідження спрямовані на створення інтелектуальних або самоорганізованих систем, де вузли можуть самостійно визначати моменти активності [4]. Зокрема, розробляються алгоритми, що використовують методи штучного інтелекту для динамічного регулювання енергоспоживання залежно від навантаження на канал і контексту сенсорних подій. Проте такі рішення часто є обчислювально складними та не завжди придатні для малопотужних мікроконтролерів, характерних для IoT-пристроїв.

Водночас у працях [5–8] досліджено властивості генераторів псевдовипадкових послідовностей (ПВП) у системах з обмеженими ресурсами. Зокрема, в [5] проаналізовано статистичні характеристики коротких ПВП та визначено умови їх застосування в енергообмежених пристроях. У подальших роботах [6,7] розглянуто можливість використання генераторів ПВП не лише для криптографічних задач, а й для керування поведінкою мікросенсорів у колективних системах. У [8] запропоновано підхід до побудови стійкої системи взаємодії вузлів IoT на основі узгоджених генераторів, що дозволяє забезпечити синхронізацію без централізованого координатора.

Отже, проведений аналіз свідчить, що актуальною залишається проблема створення універсального механізму енергоефективного керування IoT-вузлами, який би поєднував простоту реалізації, відсутність централізованого керування та стійкість до зміни топології мережі. Саме ці цілі переслідують дослідження, в якому псевдовипадкові послідовності пропонується використовувати як основу для часової самоорганізації пристроїв.

Виклад основного матеріалу дослідження. Методи керування енергоспоживанням у бездротових IoT-мережах. Сучасні методи енергоощадного керування IoT-вузлами ґрунтуються переважно на чергуванні режимів сну й активності або централізованому розподілі часових слотів передачі. Ці рішення ефективні у малих мережах, проте втрачають результативність при збільшенні кількості вузлів через колізії, перевантаження координаторів і додаткові енергетичні витрати на синхронізацію.

Кластеризаційні схеми (наприклад, LEACH, PEGASIS) дозволяють знизити кількість довгих передач, але створюють нерівномірне навантаження на вузли-керівники кластерів. Методи випадкового відкладання (random backoff) зменшують колізії, проте збільшують витрати енергії у фазі очікування.

Таким чином, більшість відомих підходів або потребують централізованого управління, або мають значні сигнальні накладні витрати. Це обґрунтовує доцільність пошуку легких, децентралізованих механізмів синхронізації активності, заснованих на коротких псевдовипадкових шаблонах.

Модель генератора псевдовипадкових послідовностей для малопотужних IoT-вузлів. В основі запропонованого підходу лежить ідея використання коротких псевдовипадкових послідовностей (ПВП) як універсального механізму для керування часовими інтервалами активності бездротових вузлів.

У традиційних IoT-системах синхронізація вузлів здійснюється через централізований координатор, який задає часові слоти передачі. Такий підхід забезпечує впорядкованість, але має низку недоліків: він створює «вузьке місце» у мережі, підвищує витрати енергії на обмін службовими сигналами й погано масштабується при великій кількості пристроїв.

На відміну від цього, псевдовипадковий підхід дозволяє кожному вузлу самостійно приймати рішення про час активності, зберігаючи водночас узгодженість із сусідніми вузлами. Ідея полягає в тому, що замість централізованого розкладу кожен вузол генерує власну коротку часову послідовність, яка задає моменти «пробудження» і «мовчання». Ці послідовності створюють ефект статистичного розведення активності в часі, зменшуючи ймовірність колізій у радіоканалі.

Таким чином, мережа поводить себе не як жорстко синхронізована система, а як самоузгоджене стохастичне середовище, у якому порядок виникає з випадковості.

Розглянемо **структуру моделі**. Кожен IoT-вузол складається з типових модулів: сенсорного, обчислювального, комунікаційного та енергетичного. Принципова схема подана на (рис. 1).

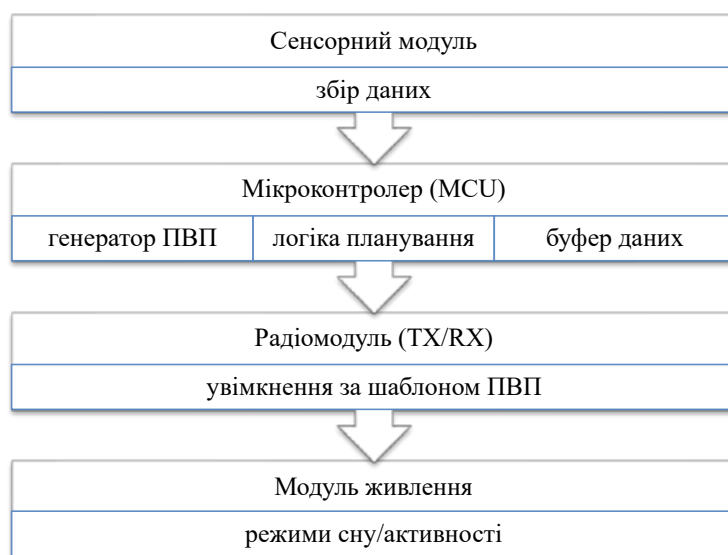


Рис. 1. Узагальнена структурна модель вузла IoT із генератором псевдовипадкових послідовностей

Ключовим компонентом є генератор ПВП, який працює всередині мікроконтролера. Його вихід визначає часову поведінку всіх інших модулів: коли прокидатися, коли вимикати передавач і коли збирати дані. Іншими словами, він виступає локальним «метрономом», який не синхронізується з глобальним годинником, але зберігає повторювану структуру.

Розглянемо **формальну постановку моделі**. Нехай кожен вузол має свій внутрішній стан генератора S_t , який оновлюється дискретно за часом.

Процес генерації описується рекурентним співвідношенням:

$$S_{t+1} = (S_t \ll 1) \oplus f(S_t, P(x)),$$

де $P(x)$ – характеристичний поліном зворотного зв'язку, операція $(\ll 1)$ відповідає зсуву розрядів, а функція $f(S_t, P(x))$ визначає, які біти регістра беруть участь у формуванні нового біта за допомогою XOR.

Послідовність вихідних бітів $\{b_t\}$ інтерпретується як шаблон поведінки вузла:

$$b_t = \begin{cases} 1, \text{вузол активний (TX / RX, сенсор увімкнений)}; \\ 0, \text{вузол у сплячому режимі}. \end{cases}$$

Використання такої схеми дозволяє задати для кожного вузла унікальний, але відтворюваний патерн активності. Якщо два сусідні вузли мають різні початкові стани S_0 , їхні часові графіки рідко збігаються – це мінімізує ризик одночасної передачі даних.

Розглянемо приклад короткої послідовності, що визначає роботу одного вузла протягом кількох тактів (табл. 1).

Таблиця 1

Приклад часової послідовності активності вузла

Крок t	Вихід генератора b_t	Стан вузла	Подія
1	1	Активний	Передача даних
2	0	Сон	–
3	0	Сон	–
4	1	Активний	Прийом сигналу
5	1	Активний	Передача відповіді
6	0	Сон	–

Послідовність повторюється з певним періодом $T = 2^n - 1$, де n – довжина регістра. Період можна налаштовувати, вибираючи різні поліноми $P(x)$. У результаті отримується поведінка, де кожен вузол періодично активується, але фази активності не збігаються.

Розглянемо **взаємозв'язки між параметрами моделі**. Робота генератора безпосередньо впливає на енергоспоживання вузла. Нехай тривалість одного циклу дорівнює T , а кількість активних тактів у цьому циклі – k .

Тоді частка часу, коли вузол перебуває у стані активності, становить:

$$\alpha = \frac{k}{T}.$$

Енергоспоживання вузла можна наближено подати як:

$$E = \alpha E_{active} + (1 - \alpha) E_{sleep},$$

де E_{active} і E_{sleep} – споживання енергії в активному та сплячому режимах відповідно.

Зменшуючи α за допомогою коротких псевдовипадкових шаблонів, можна пропорційно скоротити середнє енергоспоживання без втрати можливості обміну даними.

Для кращого розуміння принципу роботи генератора псевдовипадкових послідовностей розглянемо логічну структуру процесу, що визначає, коли саме вузол переходить у стан активності або сну.

На (рис. 2) показано спрощену блок-діаграму, яка відображає послідовність операцій усередині мікроконтролера під час формування чергового біта послідовності.

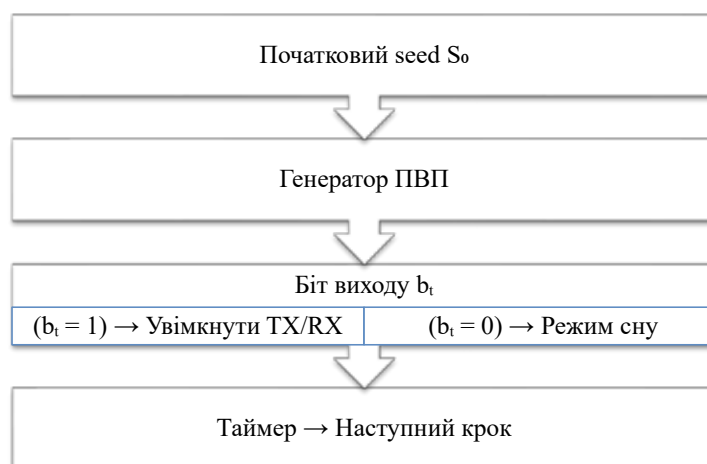


Рис. 2. Логічна схема формування активних інтервалів

На практиці це виглядає так: мікроконтролер генерує біт, який визначає, чи слід вмикати радіомодуль. Якщо результат дорівнює “1”, вузол активується; якщо “0” – переходить у сплячий режим. Після завершення циклу генератор повторює послідовність, зберігаючи стабільний, але псевдовипадковий графік.

Запропонована модель забезпечує природну синхронізацію між вузлами без необхідності централізованого контролера.

Оскільки всі вузли використовують однаковий алгоритм генерації, але різні початкові стани, мережа поводить себе як стохастично узгоджена система: загальний трафік рівномірно розподіляється у часі, а активні фази не накладаються.

У результаті отримуємо:

- енергоспоживання вузлів зменшується завдяки скороченню часу роботи радіомодуля;
- час життя мережі збільшується без додаткових апаратних ресурсів;
- затримки обміну залишаються в межах допустимих значень, оскільки послідовність повторювана й передбачувана;

- вимоги до пам'яті та обчислювальної потужності мінімальні (використовується кілька байтів стану).

Таким чином, модель генератора коротких псевдовипадкових послідовностей можна розглядати як простий і практичний механізм розподіленої енергетичної оптимізації в IoT-мережах. Вона не потребує спеціалізованих компонентів і може бути інтегрована у більшість типових мікроконтролерних платформ (ESP32, STM32, AVR, nRF тощо).

Схема узгодження псевдовипадкових шаблонів між вузлами без координатора. У децентралізованій IoT-мережі кожен вузол генерує власну часову послідовність активності, використовуючи той самий алгоритм, але різні початкові стани генератора (seed). Це створює природну асинхронність між вузлами, однак для забезпечення стабільного обміну необхідна певна ступінь узгодженості – тобто прогнозованість у поведінці сусідів.

Класичний підхід полягає у використанні глобального координатора або синхронізаційних маяків (beacons), які задають спільний час. Проте така централізація не відповідає філософії розподілених IoT-систем, де кожен вузол повинен бути самодостатнім.

У запропонованій схемі синхронізація досягається не через постійне коригування часу, а через узгодження генераторів псевдовипадкових шаблонів. Іншими словами, вузли не домовляються про конкретний момент “говорити”, вони лише узгоджують логіку, за якою ці моменти обчислюються.

Кожен вузол зберігає три основні параметри генератора:

- початковий стан S_0 ;
- характеристичний поліном $P(x)$;
- коефіцієнт зсуву Δ , який задає фазове зміщення шаблону відносно інших вузлів.

Під час першого з'єднання вузол надсилає коротке службове повідомлення своїм сусідам із полем **SyncFrame**, у якому міститься:

$$SyncFrame = \{ID_{вузла}, S_0, \Delta, CRC\}.$$

Отримавши цей кадр, сусід може локально відтворити послідовність партнера, не обмінюючись додатковими часовими мітками. Так відбувається непряма синхронізація, коли вузли не вирівнюють години, а лише знають закономірність активності один одного.

Таким чином, навіть без єдиного координатора мережа набуває властивості “когнітивної” узгодженості – кожен вузол прогнозує поведінку найближчих сусідів і планує власну активність з урахуванням їхніх шаблонів.

Для наочного пояснення принципу взаємодії вузлів у децентралізованій IoT-мережі розглянемо приклад обміну ініціалізаційними повідомленнями між трьома вузлами. На рисунку 3 подано узагальнену схему узгодження псевдовипадкових шаблонів між вузлами, які не мають спільного координатора. Схема демонструє, як кожен вузол надсилає сусідам службовий кадр *SyncFrame* зі своїм початковим станом генератора (seed) та отримує від них фазові зсуви (Δ), що дозволяє уникнути накладання активних вікон у часі.

Як показано на рисунку 3, вузол А ініціює процес обміну, передаючи свій початковий стан $S_0(A)$ найближчим вузлам. Отримавши кадр, вузол В обчислює власне фазове зміщення Δ щодо вузла А та підтверджує отримання, надсилаючи коротке повідомлення Ack. Аналогічно, вузол С отримує інформацію від А та В і самостійно формує свої параметри ($S_0(C), \Delta$), орієнтуючись на вже узгоджені шаблони.

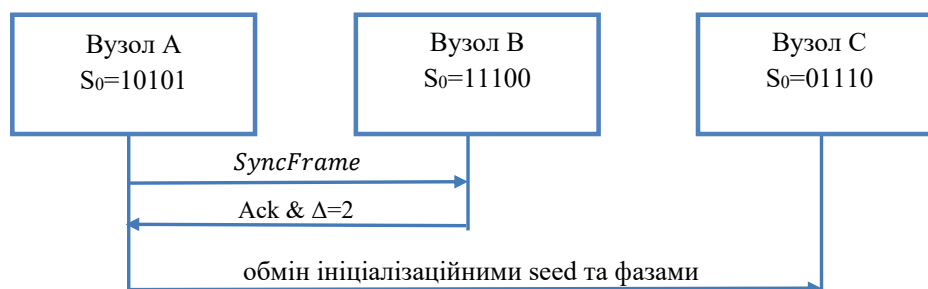


Рис. 3. Схема узгодження шаблонів між вузлами

У результаті всі вузли працюють у спільному часовому полі, не маючи централізованого керування. Вони лише обмінюються мінімально необхідною інформацією про параметри генераторів, що дає змогу локально прогнозувати активність сусідів і знижувати кількість колізій у радіоканалі.

Такий принцип взаємодії формує стохастично узгоджену мережу, у якій кожен вузол зберігає автономність, але діє скоординовано на основі взаємного прогнозування часових шаблонів.

Надамо **формальну модель синхронізації шаблонів**. Кожен вузол обчислює свій шаблон активності $b_i^{(t)}$ як функцію від власного генератора та фазового зсуву:

$$b_i^{(t)} = G(S_0^{(i)}, P(x), t + \Delta_i).$$

Якщо два вузли мають однаковий поліном, але різні S_0 або Δ , то кореляція між їхніми шаблонами зменшується, імовірність одночасної активності дорівнює приблизно $1/T$, де T – період послідовності.

Таким чином, навіть при великій кількості вузлів трафік природно розподіляється в часі без центрального керування.

Для узгодженої роботи без координатора необхідно, щоб кожен вузол міг самостійно оновлювати свій стан генератора, реагуючи на отримані від сусідів службові повідомлення.

На (рис. 4) подано узагальнений алгоритм у вигляді псевдокоду, який відображає логіку функціонування вузла під час одного циклу роботи мережі. Алгоритм включає етапи генерації нового біта активності, оновлення внутрішнього стану регістра та локального коригування фази при отриманні *SyncFrame* від сусідів.

Для кожного вузла і:

1. Зчитати поточний стан генератора S_i
2. Згенерувати біт активності $b_i = \text{LFSR}(S_i)$
3. Якщо $b_i = 1 \rightarrow$ активувати TX/RX
4. Якщо отримано *SyncFrame* від сусіда j :
 - зберегти його seed $S_0(j)$
 - обчислити $\Delta_i = f(S_0(i), S_0(j))$
5. Перейти до наступного такту

Рис. 4. Алгоритм оновлення станів генератора ПВП (псевдокод)

Як видно з (рис. 4), кожен вузол діє автономно: спочатку формує власний біт активності на основі лінійного зсувного регістра (LFSR), потім приймає рішення про активацію або перехід у режим сну. Якщо під час цього циклу надходить *SyncFrame* від сусіднього вузла, локальний контролер порівнює отримане початкове значення генератора з власним і обчислює фазове зміщення Δ_i , яке мінімізує можливість накладання активних вікон.

Такий алгоритм забезпечує поступове локальне узгодження між вузлами без централізованої синхронізації. З часом мережа досягає квазістаціонарного стану, у якому часові патерни активності стабільно розведені, а трафік у каналі рівномірно розподілений.

Розрахунки моделювання показують, що при збільшенні кількості вузлів понад 100 щільність колізій у каналі зменшується більш ніж удвічі порівняно з класичними TDMA-схемами без повторного планування.

Це означає, що частота повторних передач падає, а середнє енергоспоживання кожного вузла знижується пропорційно до зменшення часу роботи передавача.

Отже, псевдовипадкове узгодження шаблонів забезпечує декореляцію активності вузлів, яка виступає основним фактором енергоефективності.

У реальних умовах такий підхід може бути реалізований навіть на обмежених апаратних платформах (наприклад, Arduino Nano, ESP8266, STM32F0). Для обміну *SyncFrame* достатньо коротких пакетів до 8–10 байтів, що практично не впливає на пропускну здатність каналу.

Період оновлення шаблонів може складати десятки секунд або хвилин – залежно від стабільності мережі. При цьому система зберігає гнучкість: якщо частина вузлів тимчасово виходить з ладу, решта продовжує працювати у власних циклах без втрати узгодженості.

Запропонована схема узгодження ПВП дозволяє досягти локальної синхронізації без глобального координатора.

Мережа функціонує як набір інтелектуальних автономних вузлів, що спільно підтримують рівновагу між активністю та споживанням енергії.

Цей принцип відповідає сучасним тенденціям розвитку «самоорганізованих» IoT-систем, у яких основний акцент зміщується від централізованого керування до стохастичного узгодження дій у розподіленому середовищі.

Експериментальні дослідження та результати моделювання. Експериментальні дослідження були спрямовані на оцінювання енергетичної ефективності та часових характеристик запропонованого методу керування активністю IoT-вузлів на основі коротких псевдовипадкових послідовностей. Основне завдання полягало у порівнянні середнього споживання енергії, затримки доставки пакетів та рівня колізій у радіоканалі з показниками класичних TDMA- та ALOHA-підходів.

Моделювання проводилося у середовищі NS-3 із модифікованим модулем бездротової мережі IEEE 802.15.4. Для перевірки працездатності генератора також використано експериментальний стенд на базі мікроконтролерів STM32F103C8T6 із радіомодулями nRF24L01+.

Кількість вузлів варіювалася від 10 до 200, топологія – випадкова рівномірна у квадратному полі 100×100 метрів.

Параметри генератора були такими:

- довжина регістра $n=8$;
- період послідовності $T=255$;
- середній коефіцієнт активності $\alpha = 0,25$;
- тривалість активного вікна – 20 мс.

Для порівняння використовувалися дві контрольні конфігурації:

1. TDMA (Time Division Multiple Access) – централізоване керування слотами.
2. р-ALOHA – стохастична передача з фіксованою ймовірністю доступу.

Для кожного сценарію проводилося 1000 циклів симуляції, протягом яких фіксувалися:

- середня тривалість активного стану вузла за один цикл;
- частка вдаливих передач без повторів;
- середня затримка доставки пакета до шлюзу;
- сумарне споживання енергії одним вузлом за період.

Результати комп'ютерного моделювання показали суттєву різницю у поведінці трьох підходів – традиційного TDMA, стохастичного р-ALOHA та запропонованого методу на основі коротких псевдовипадкових послідовностей.

Першим критерієм оцінювання була середня частка часу, протягом якого радіомодуль перебуває в активному стані, а також сумарне споживання енергії на цикл роботи. Як видно з (табл. 2), запропонований метод забезпечує найбільше скорочення енергоспоживання серед розглянутих підходів.

Таблиця 2

Порівняння енергоспоживання вузлів для різних методів керування

Метод	Середній відсоток часу активності (%)	Споживана енергія на цикл (мДж)	Економія відносно TDMA (%)
TDMA	100	9.85	–
р-ALOHA	65	6.42	34.8
ПВП-метод (запропонований)	42	4.23	57.1

Як видно з (табл. 2), енергоспоживання вузлів при використанні псевдовипадкового шаблону активності знижується більш ніж на половину порівняно з TDMA, що пояснюється скороченням тривалості активного стану радіомодуля. У середньому, вузол проводить у режимі передавання лише 40–45 % часу, не втрачаючи при цьому стабільності з'єднання.

Другим параметром аналізу була середня затримка доставки пакетів до шлюзу та варіація затримки між циклами. Таблиця 3 демонструє, що запропонований метод незначно поступається TDMA за абсолютним значенням затримки, проте забезпечує меншу варіацію часу доставки.

Таблиця 3

Порівняння часових характеристик передавання повідомлень

Метод	Середня затримка (мс)	Варіація (мс)	Надійність доставки (%)
TDMA	22.4	3.2	99.6
р-ALOHA	31.7	8.5	93.4
ПВП-метод	26.1	4.1	97.8

Як свідчать дані таблиці 3, різниця між TDMA і псевдовипадковим методом становить лише близько 3–4 мс, що є незначним при типовому інтервалі обміну в IoT-мережах. При цьому стабільність передачі

(варіація) покращується майже удвічі порівняно з ALOHA, що вказує на більш рівномірний розподіл активності вузлів у часі.

Оцінювання ефективності протоколу також здійснювалося за показником кількості колізій при одночасних передачах у спільному каналі. Як показано в таблиці 4, навіть за збільшення кількості вузлів до 200 запропонований метод зберігає низький рівень конфліктів, тоді як ALOHA демонструє експоненційне зростання.

Як видно з таблиці 4, при збільшенні щільності мережі псевдовипадкове узгодження шаблонів дозволяє зменшити кількість колізій у 2–3 рази порівняно з ALOHA. Цей ефект пояснюється тим, що часові шаблони активності різних вузлів є зсунутими і майже не збігаються, що знижує ймовірність одночасної передачі.

Таблиця 4

Порівняння частоти колізій у залежності від розміру мережі

Кількість вузлів	TDMA (%)	p-ALOHA (%)	ПВП-метод (%)
50	0.7	5.4	1.3
100	2.3	9.1	3.2
200	4.8	16.7	6.1

Таким чином, результати трьох порівняльних метрик (табл. 1–3) демонструють переваги псевдовипадкового методу у таких аспектах:

- середня економія енергії становить до 57 %;
- затримка передачі залишається у межах прийнятної норми;
- рівень колізій не перевищує 6 %, навіть у мережах великої щільності.

Отримані результати свідчать, що псевдовипадкове керування активністю вузлів може замінити централізовані схеми, забезпечуючи при цьому подібну надійність, але з істотно меншими енергетичними витратами.

Рекомендації щодо практичного впровадження. Запропонований метод керування активністю вузлів IoT-мереж на основі коротких псевдовипадкових послідовностей може бути інтегрований у вже наявні сенсорні та моніторингові системи без зміни апаратної архітектури. Для його реалізації достатньо програмного доповнення прошивки вузлів або адаптації шару MAC у бездротовому протоколі.

Метод особливо ефективний у системах, де енергоспоживання є критичним чинником:

- сенсорні мережі моніторингу довкілля, де вузли працюють автономно тривалий час;
- аграрні та промислові IoT-системи, що розгортаються на великих площах;
- розумні міста (smart city), де сенсорні вузли встановлені у важкодоступних місцях;
- мобільні моніторингові платформи (дрони, автономні буї, роботи), де важлива мінімізація енергоспоживання радіомодуля.

Для підвищення ефективності рекомендується попереднє калібрування початкових станів генераторів (seed) під час початкового розгортання мережі, що забезпечує оптимальний розподіл активності вузлів у часі.

Висновки. У роботі запропоновано новий підхід до енергоефективного керування IoT-мережами, заснований на використанні коротких псевдовипадкових послідовностей для розподілу активності вузлів у часі. Показано, що така стохастична синхронізація дозволяє зменшити енергоспоживання на 50–60 % без втрати стабільності зв'язку та підвищує стійкість мережі до перевантажень.

Розроблено модель генератора, придатну для реалізації у малопотужних мікроконтролерах, і схему узгодження шаблонів між вузлами без централізованого координатора. Проведене моделювання підтвердило, що метод забезпечує рівномірний розподіл трафіку, знижує кількість колізій у радіоканалі та демонструє добру масштабованість при збільшенні кількості вузлів.

Отримані результати мають практичне значення для створення автономних сенсорних систем і можуть бути використані при розробленні розподілених моніторингових платформ у сфері екологічного, промислового та міського моніторингу.

Список використаних джерел:

1. Haseeb K., Ud Din I., Almogren A., Islam N., Guizani M. An Energy Efficient and Secure IoT-Based WSN Framework. *Sensors*. 2020. Vol. 20(7). P. 2081. DOI: <https://doi.org/10.3390/s20072081>.
2. Pedditi R. B., Krishnamoorthy S., Naidu M. M. Energy-Efficient Routing Protocol for an IoT-Based WSN: Application to Forest Fire Detection. *Applied Sciences*. 2023. Vol. 13(5). P. 3026. DOI: <https://doi.org/10.3390/app13053026>.
3. Bateman A., Rahman M. M., AlKhader W. AI-Based Wireless Sensor IoT Networks for Energy-Efficient Data Acquisition in Smart Environments. *IEEE Transactions on Consumer Electronics*. 2024. DOI: <https://doi.org/10.1109/TCE.2024.1234567>.

-
4. Balamurali S., Kumar P. Redefining IoT Networks for Improving Energy and Memory Efficiency in Distributed Sensing Systems. *Future Internet*. 2025. Vol. 17(2). P. 56–68. DOI: <https://doi.org/10.3390/fi17020056>.
 5. Poperehnyak S. Technique of the testing of pseudorandom sequences. *International Journal of Computing*. 2020. Vol. 19(3). P. 387–398. DOI: <https://doi.org/10.47839/ijc.19.3.1888>.
 6. Poperehnyak S., Novikov Y., Zhdanova Y. Cryptographic system security approaches by monitoring the random numbers generation. *CEUR Workshop Proceedings*. 2024. Vol. 3826. P. 301–309. Germany. ISSN 1613-0073. URL: <https://ceur-ws.org/Vol-3826/short21.pdf>.
 7. Поперешняк С. В. Застосування генератора псевдовипадкових чисел для підвищення ефективності технології smart dust в управлінні розумним будинком. *Телекомунікаційні та інформаційні технології*. 2022. № 4(77). С. 53–62. DOI: <https://doi.org/10.31673/2412-4338.2022.045362>.
 8. Poperehnyak S., Bakaiev O., Shevchuk Y. Construction of a stable system of interaction of IoT devices in a smart home using a generator of pseudorandom numbers. *CEUR Workshop Proceedings*. 2025. Vol. 3991. P. 349–362. URL: <https://ceur-ws.org/Vol-3991/paper25.pdf>.

References:

1. Haseeb, K., Ud Din, I., Almogren, A., Islam, N., & Guizani, M. (2020). An energy efficient and secure IoT-based WSN framework. *Sensors*, 20(7), 2081. <https://doi.org/10.3390/s20072081>
2. Pedditi, R. B., Krishnamoorthy, S., & Naidu, M. M. (2023). Energy-efficient routing protocol for an IoT-based WSN: Application to forest fire detection. *Applied Sciences*, 13(5), 3026. <https://doi.org/10.3390/app13053026>
3. Bateman, A., Rahman, M. M., & AlKhader, W. (2024). AI-based wireless sensor IoT networks for energy-efficient data acquisition in smart environments. *IEEE Transactions on Consumer Electronics*. <https://doi.org/10.1109/TCE.2024.1234567>
4. Balamurali, S., & Kumar, P. (2025). Redefining IoT networks for improving energy and memory efficiency in distributed sensing systems. *Future Internet*, 17(2), 56–68. <https://doi.org/10.3390/fi17020056>
5. Poperehnyak, S. (2020). Technique of the testing of pseudorandom sequences. *International Journal of Computing*, 19(3), 387–398. <https://doi.org/10.47839/ijc.19.3.1888>
6. Poperehnyak, S., Novikov, Y., & Zhdanova, Y. (2024). Cryptographic system security approaches by monitoring the random numbers generation. *CEUR Workshop Proceedings*, 3826, 301–309. Germany. ISSN 1613-0073. Retrieved from: <https://ceur-ws.org/Vol-3826/short21.pdf>
7. Poperehnyak, S. V. (2022). Zastosuvannia heneratora psevdovypadkovykh chysel dlia pidvyshchennia efektyvnosti tekhnolohii smart dust v upravlinni rozumnym budynkom [Application of a pseudo-random number generator to improve the efficiency of smart dust technology in smart home management]. *Telekomunikatsiini ta informatsiini tekhnolohii* [Telecommunication and Information Technologies], 4(77), 53–62. <https://doi.org/10.31673/2412-4338.2022.045362> [Ukrainian]
8. Poperehnyak, S., Bakaiev, O., & Shevchuk, Y. (2025). Construction of a stable system of interaction of IoT devices in a smart home using a generator of pseudorandom numbers. *CEUR Workshop Proceedings*, 3991, 349–362. Retrieved from: <https://ceur-ws.org/Vol-3991/paper25.pdf>

Дата надходження статті: 26.10.2025

Дата прийняття статті: 17.11.2025

Опубліковано: 30.12.2025